PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q

A2

(11) International Publication Number: WO 99/48303

(43) International Publication Date: 23 September 1999 (23.09.99)

(21) International Application Number: PCT/US99/05900

(22) International Filing Date: 18 March 1999 (18.03.99)

(30) Priority Data:
09/040,898 18 March 1998 (18.03.98) US

(71) Applicant: CISCO TECHNOLOGY, INC. [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventors: COX, Dennis; 6800 McNeil Drive #828, Austin, TX 78729 (US). MCCLANAHAN, Kip; 3112 Kerbey Lane, Austin, TX 78703 (US).

(74) Agent: SHOWALTER, Barton, E.; Baker & Botts, L.L.P., 2001 Ross Avenue, Dallas, TX 75201-2980 (US).

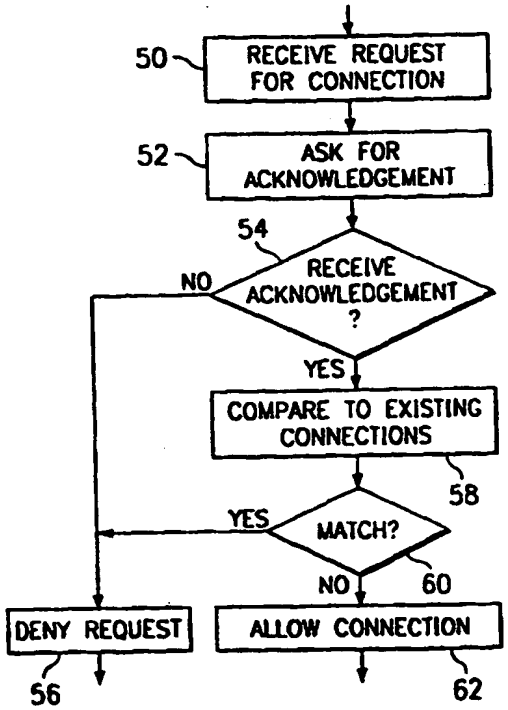
(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD FOR BLOCKING DENIAL OF SERVICE AND ADDRESS SPOOFING ATTACKS ON A PRIVATE NETWORK

(57) Abstract

A method is provided for blocking attacks on a private network (12). The method is implemented by a routing device (10) interconnecting the private network (12) to a public network (14). The method includes analyzing an incoming data packet from the public network (14). The incoming data packet is then matched against known patterns where the known patterns are associated with known forms of attack on the private network (12). A source of the data packet is then identified as malicious or non-malicious based upon the matching. In one embodiment, one of the known forms of attack is a denial of service attack and an associated known pattern in unacknowledged data packets. In another embodiment, one of the known forms of attack is an address spoofing attack and an associated known pattern is a data packet having a source address matching an internal address of the private network (12).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

METHOD FOR BLOCKING DENIAL OF SERVICE AND ADDRESS SPOOFING ATTACKS ON A PRIVATE NETWORK

TECHNICAL FIELD OF THE INVENTION

This invention relates in general to communication systems, and more particularly to a method for blocking denial of service and address spoofing attacks on a private network.

BACKGROUND OF THE INVENTION

Corporate and other private networks often provide external access outward and inward through Internet gateways, firewalls or other routing devices. It is important for these routing devices to defend the private network against attackers from the outside as well as to allow access to the private network by authorized users. However there are numerous forms of attack on conventional routing device that can incapacitate the devices and interfere with an associated private network. The problem of keeping unauthorized persons from accessing data is a large problem for corporate and other information service management. Routing devices, such as gateways, firewalls and network routers lack important safeguards to block or prevent attacks. In particular, the number of denial service attacks have risen dramatically in recent years. Further, IP spoofing incidents occur with increasing frequency.

A denial of service attack consists of repeatedly sending requests for connections to different hosts through and/or behind the routing device. Typically, the host will wait for acknowledgment from the requester.

Because a host can only handle a finite number of requests (for example, 1 to n, where n depends on the resources available to the host), the attacker can crash or "flood" a host with requests to the point of disrupting network service (host/server/port) to users.

Another form of attack is address spoofing which can be used by unauthorized third parties to gain access to a private network. This attack involves the attacker identifying a valid internal network address within the private network. The attacker then requests access to the private network through the routing device by spoofing that internal network address. Conventional routing devices typically are not sophisticated enough to determine that such a request should be denied (i.e., because an external request can not originate from an internal address) and will allow access to the attacker. Address spoofing attacks can be carried out against various types of networks and network protocols such as IPX/SPX, MAC layer, Netbios, and IP.

It is therefore advantageous to provide facilities within a routing device that block denial of service, address spoofing and other attacks on an associated private network.

SUMMARY OF THE INVENTION

In accordance with the present invention, a method for blocking denial of service and address spoofing attacks on a private network is disclosed that provides significant advantages over conventional network routing devices.

According to one aspect of the present invention, the method is implemented by a routing device interconnecting the private network to a public network. The method includes analyzing an incoming data packet from the public network. The incoming data packet is

then matched against known patterns where the known patterns are associated with known forms of attack on the private network. A source of the data packet is then identified as malicious or non-malicious based upon the matching. In one embodiment, one of the known forms of attack is a denial of service attack and an associated known pattern is unacknowledged data packets. In another embodiment, one of the known forms of attack is an address spoofing attack and an associated known pattern is a data packet having a source address matching an internal address of the private network.

A technical advantage of the present invention is the enabling of a routing device to the identify a denial of service attack and to block such an attack from tying up the routing device.

Another technical advantage of the present invention is enabling a routing device to identify an address spoofing attack and to block such an attack.

A further technical advantage of the present invention is an ability for the routing device to track information about the attacker to allow preventive measures to be taken.

Other technical advantages should be readily apparent to one skilled in the art from the following figures, description, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention and advantages thereof may be acquired by referring to the following description taken in conjunction with the accompanying drawings, in which like reference numbers indicate like features, and wherein:

FIGURE 1 is a block diagram of an communication system including a routing device and an associated private network;

FIGURE 2 is a flow chart of one embodiment of a method for blocking attacks on a private network according to the present invention;

FIGURE 3 is a flow chart of one embodiment of a method for blocking an address spoofing attack according to the present invention; and

FIGURE 4 is a flow chart of one embodiment of a method for blocking a denial of service attack according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 is a block diagram of an communication system including a routing device 10 and an associated private network 12. Routing device 10 provides a connection between corporate private network 12 and an Internet cloud 14. Routing device 10 can include a gateway, firewall or other device interconnecting private network 12 and Internet cloud 14. In operation, routing device 10 allows internal users within private network 12 to gain access to Internet cloud 14. Routing device 10 also allows external users connected to Internet cloud 14 to gain access to private network 12. A significant and growing problem is that an attacker 16 may try to gain access to or disrupt private network 12 through Internet cloud 14.

Denial of service and address spoofing are two common forms of attack that might be used by attacker 16. In general, a denial service attack is one in which attacker 16 attempts to prevent others from using private network 12. A denial service attack works if routing device 10 spends all of its time processing requests and cannot respond quickly enough to satisfy additional requests. An Address spoofing attack is on in which attacker 16 fakes an internal address to get around or into standard address filtering schemes. According to

the present invention, routing device 10 is enabled with a method for blocking these and other types of attacks by analyzing incoming data packets.

Thus, one possible occurrence is that attacker 16 will try to get into private network 12 by spoofing an address that exists inside private network 12. This is intended to allow attacker 16 to gain access and impersonate an internal user. When a packet from attacker 16 reaches routing device 12, an attack blocking component, according to the present invention, will notice that the address matches one that exists within private network 12. Because incoming packets should not be the same as outgoing packets, the attack blocking component can deny access to private network 12 and record the information about the attack for use by the system administrator. Attacker 16 can also try to deny access to all external users by conducting a denial of service attack. This involves attacker 16 flooding private network 12 or routing device 10 by sending an extremely large number of packets. For example, attacker 16 may send 30,000 or more packets. According to the present invention, the attack blocking component of routing device 10 can notice that the first packet is spoofed or that it cannot be acknowledged and ignore all other packets. Further, routing device 10 can use diagnostic detection tools (e.g., trace root, ping, NS lookup) to pinpoint attacker 16 and notify the system administrator. In general, according to the present invention, routing device 10 can be enabled to intelligently analyze incoming packets, match the packets against known patterns for attack strategies and respond accordingly to malicious packets.

FIGURE 2 is a flow chart of one embodiment of a method for blocking attacks on a private network according to the present invention. As shown, an

incoming packet is analyzed by the routing device in step 20. In step 22, the routing device analyzes the incoming packet against known patterns. Based upon this pattern matching, in step 24, the routing device can identify the data packet and its source as malicious or non-malicious. The known patterns used in step 22 can be built using knowledge about various types of attacks. This knowledge can be recorded in the form of patterns that are then stored in a database or other storage device accessible by the routing device. The routing device can then match the analyzed packets against the patterns to determine whether or not some type of attack is being made. If an attack is identified, the routing device can identify the source of that packet as malicious and treat the source accordingly.

In particular, the routing device can implement methods for blocking denial of service attacks and address spoofing attacks as shown, for example, in FIGUREs 3 and 4. FIGURE 3 is a flow chart of one embodiment of a method for blocking an address spoofing attack according to the present invention. This method is applicable to address spoofing attacks on various types of networks, but is described speficially with respect to an IP network.

As shown in step 30 of FIGURE 3, the routing device receives a packet. In step 32, the routing device compares the IP address of the packet against known internal IP addresses of the associated private network. In step 34, the routing device determines if the source IP address matches an internal address. If not, in step 36, the routing device routes the packet as appropriate for the packet. However, if the source IP address matches an internal address, then the routing device identifies that there is an attempt to spoof an internal address. The addressed is known to be spoofed because an

internal IP address of the private network cannot be accessing the private network from an external point. Consequently, in step 38, the routing device drops the packet and does not route it to the network. In step 40, the routing device analyzes the packet header for the history of the packet in order to obtain some information about the source of the packet. Then, in step 42, the routing device takes an appropriate defensive action against that packet. For example, the routing device can refuse to accept any more packets from the real source of the packet. In this case, the defensive action can include adding the offending IP address to a cache of IP addresses and then not allowing access to the router device for any IP address in the cached list. Further, the routing device can store information about the attack for later use and for analysis for administrators of the private network. For example, information concerning the packet origination, destination or content can be stored internally to the router device or sent to a syslog server for later analysis.

FIGURE 4 is a flow chart of one embodiment of a method for blocking a denial of service attack according to the present invention. As shown, in step 50, the routing device receives a request for a connection. Then, in step 52, the routing device asks for an acknowledgment from the requestor. In step 54, the routing device checks whether or not an acknowledgment has been received. If one is not received within a specified period of time, the routing device moves to step 56 and denies the request. This denial ensures that the routing device does not churn on pending requests even though acknowledgments have not been received within reasonable amounts of time.

If an acknowledgment is received in step 54, the routing device moves to step 58 and compares the

requested connection to existing connections. Then, in step 60, the routing device determines if there is a match between the requested connection and one of the existing connections. If so, the routing device moves to step 46 and denies the request. The request is denied because one source should not have more than one connection through the routing device to the private network. If, in step 60, there is no match, then the routing device can allow the connection in step 62. The method of FIGURE 4 prevents the routing device from being tied up by multiple requests from one source and thereby blocks the denial of service attack.

In general, the method of the present invention can be integrated as a component of a gateway, firewall or other routing device. In one implementation, the present invention can work off of a variable size cache file that holds network addresses. For blocking spoofing, each incoming address can be held in the cache file and checked to see if the incoming address matches an network address that is on the private network. If the incoming address matches, then the request can be denied. Also, a message can be sent to a system log which, rather than being written to a file, can be written to a console to prevent the log from getting overloaded and crashing the routing device. Further, an optional E-mail message or page can be sent to a specified address or number in the case of an attack. If an attack happens more than once on the same address in the span of a certain period of time (for example, five minutes), then the number of messages can be limited to prevent overloading of the E-mail or paging service. An optional shutdown mechanism can also be in place that will enable the routing device to automatically shut down certain services if attacks continued.

Denial of service attacks are generally easier to trace. However, when such an attack is also spoofed, the problem becomes very difficult to stop. According to the present invention, an incoming address can be checked against the cache file and a quick search can be performed to see if the address is already in a list of pending addresses. If so, the request packet can be discarded. An address is removed from the list if a successful acknowledge packet is sent back or a variable time limit is reached. The number of matching addresses that are allowed in the list can be a variable set by the system administrator.

Although the present invention has been described in detail, it should be understood that various changes, substitutions and alterations can be made thereto without departing from the sphere and scope of the invention as defined by the appended claims.

WHAT IS CLAIMED IS:

1. A method for blocking attacks on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

analyzing an incoming data packet from the public network;

matching the incoming data packet against known patterns, the known patterns associated with known forms of attack on the private network; and

identifying a source of the data packet as malicious or non-malicious based upon the matching.

2. The method of Claim 1, wherein one of the known forms of attack is a denial of service attack and an associated known pattern is unacknowledged data packets.

3. The method of Claim 1, wherein one of the known forms of attack is an address spoofing attack and an associated known pattern is a data packet having a source address matching an internal address of the private network.

4. The method of Claim 1, wherein the public network is the Internet.

5. The method of Claim 4, wherein the routing device is a firewall providing access to the Internet.

6. A method for blocking an address spoofing attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

receiving an incoming data packet from the public network;

comparing a source address of the data packet against known internal addresses of the private network;

determining if the source address matches a known internal address;

if there is no match, routing the data packet to the private network;

if there is a match, dropping the data packet.

7. The method of Claim 6, further comprising, if there is a match, analyzing a header of the data packet for a history of the data packet and taking defensive action against the data packet based upon the history.

8. The method of Claim 7, wherein the defensive action comprises refusing to accept any more data packets from a real source of the data packet.

9. The method of Claim 7, wherein the defensive action comprises storing information about the data packet for use and analysis by a system administrator.

10. The method of Claim 6, wherein the public network is the Internet.

11. The method of Claim 10, wherein the routing device is a firewall providing access to the Internet.

12. A method for blocking a denial of service attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

receiving a request for a connection from the public network;

requesting an acknowledgment from an initiator of the request;

determining whether an acknowledgment has been received;

if an acknowledgment is not received, denying the request;

if an acknowledgment is received, comparing the request to existing connections;

if there is a match between the request and an existing connection, denying the request;

if there is not match between the request and an existing connection, allowing the connection and routing packets to the private network.

13. The method of Claim 12, wherein the public network is the Internet.

14. The method of Claim 13, wherein the routing device is a firewall providing access to the Internet.

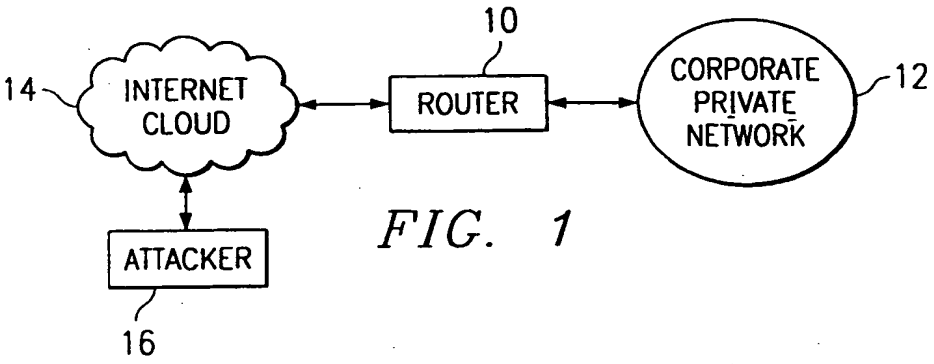


FIG. 1

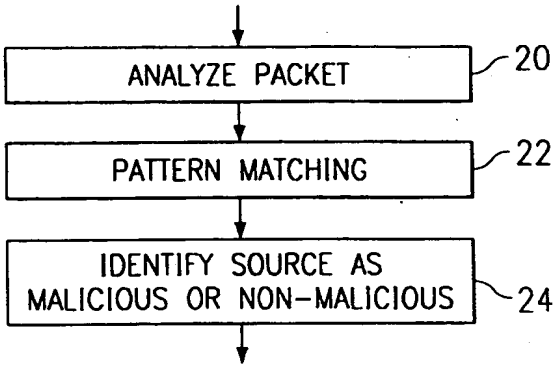


FIG. 2

FIG. 3

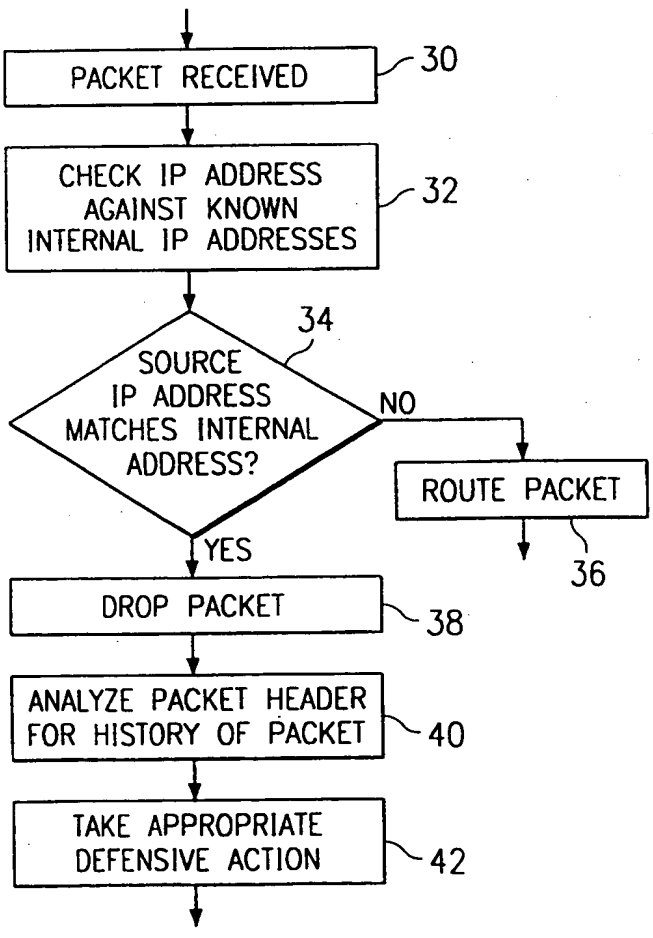
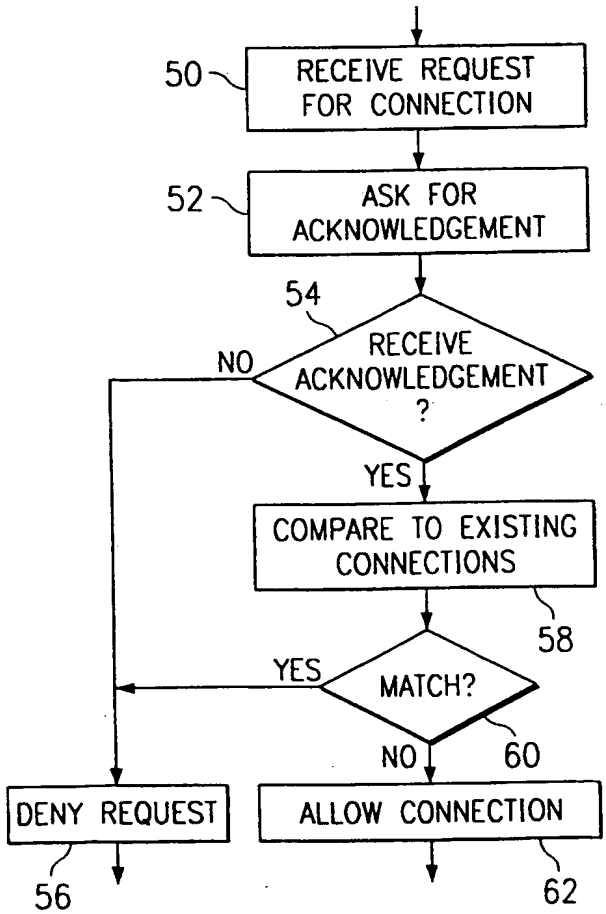


FIG. 4



THIS PAGE BLANK (USPTO)